Protecting the IIoT Infrastructure

The Great DRAM-Firewall

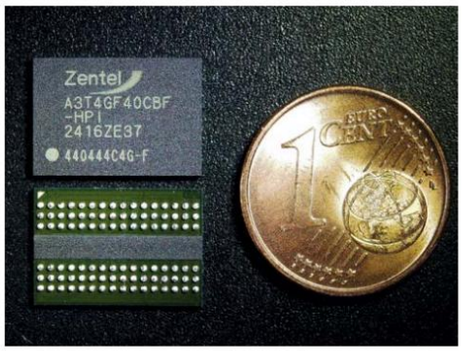
Zentel recently qualified its Row Hammer-immunized DDR3 DRAM chip with integrated error correction code (ECC) for Automotive Grade 2 – not primarily for cars, but to protect its own power grids from hostile cyber attacks.

Since the spread of the third DDR DRAM generation ten years ago It became public that DDR3 DRAMs in IoT systems represent a latent vulnerability and a potential gateway via the hardware for disguised cyber attacks from the Internet using extremely sophisticated manipulated websites - even bypassing all relevant software-based protective measures such as firewalls, antivirus apps or operating system patches, and without leaving any forensic traces in the volatile main memory: "no smoking gun".

Since then, there has been a never-ending game of cat and mouse between the DRAM industry and a highly professional hacker elite. This includes professors at ETH Zurich and their research teams such as "SAFARI" led by Prof. Onur Mutlu and the Computer Security Group led by Prof. Kaveh Razavi.

Just recently, the SAFARI publication “RowPress: Amplifying Read Disturbance in Modern DRAM Chips” was named the top pick of last year by the journal IEEE Micro.
It was revealed that even newer DRAM generations are not immune to row hammer attacks, especially if the activation range for targeted attacks is too short.

Pictures:



The row hammer protected 4 Gbit DDR3L DRAM IC »A3T4GF40CBF-HP« with integrated error correction code and proprietary bit flip overflow alarm for the controller is now available in automotive grade 2 to protect power grids from cyber attacks.

ne data rows is significantly expanded. In the RowPress paper, it is shown that the Row- Hammer-prone cells do not overlap with the Row- Press-prone cells, so this effect is "Row-Hammer-like".

The DRAM industry had hoped in vain to outmaneuver cyber attacks by introducing a Target Row Refresh (TRR) that was possible for the first time with the DDR4-JEDEC standard and "shell game tricks" - by proprietary concealment of the physical data row addresses . In May 2020, the research team presented "VUSec" under authoritative

With the help of Kaveh Razavi at the Vri-je Universiteit Amsterdam, the paper "TRRespass: Exploiting the Many Sides of Target Row Refresh" was published at the "IEEE Symposium on Security and Privacy" held virtually due to the pandemic. This paper was able to circumvent the hide-and-seek game in DDR4 DRAMs from the three leading manufacturers (with 94 percent global market coverage) using an FPGA-based fuzzing algorithm. An earlier paper "RAMBleed: Reading Bits in Memory Without Accessing Them" also shook up the scientific community by showing that in DDR3 DRAMs from all top 3 manufacturers, a target row refresh that was actually generated by the operating system could be exploited.

The system was able to remotely read the RSA-2048 decryption code hidden in locked memory areas and passwords with a row hammer attack on more than one line of data - including in smartphones - and hijack entire networks with the spied-out administrator rights.

Final acid test for first Row-Hammer-protected DDR3-DRAM-ICs

In the meantime, Kubo Takashi, CTO of Zentel in Japan, had developed 2 Gbit and 4 Gbit DDR3L chips with a new type of integrated row hammer watchdog and capture circuit made up of counter tree and SRAM structures. However, they were not suitable for DDR4 DRAM ICs with their typically higher storage densities . Because of the disproportionately higher additional chip area required and a correspondingly lower wafer yield , they would be so expensive that they would be unsellable in the merciless DRAM price competition . This cost disadvantage also applies to protected DDR3L ICs, but within a less price-critical framework. There are still many ambitious IoT applications, even in connection with UHD displays or correspondingly high-resolution digital cameras, for which DDR4 DRAMs with their higher clock rates and storage densities would be overkill . The requirement for an additional capture circuit originally came from the HDD/SSD industry to protect the DRAM cache from data corruption or spying. The ETH COMSEC team led by Prof. Kaveh Razavi relied on Kubo Takshi's industrial expertise , among other things, in the development of an ultimately more stringent test algorithm with the working title "Blacksmith: Scalable Rowhammering in the Frequency Domain". As an advisory supporter of the team from the industrial DRAM chip design perspective and co-author of various publications, he had access to the test algorithm for DDR4 DIMM modules and ported it to an automatic test equipment for his row hammer protected DDR3L DRAM ICs to ensure that they also withstood this final, more stringent row hammer test.

The Hardware Cybersecurity Dilemma – Two Sides of the Same Coin

In June 2024, Prof. Kaveh Razavi spoke at the Cyb3r Spotlight Event in Oerlikon on the state of hardware cybersecurity research with his lecture "How I learned to stop worrying and love the insecure hardware," apparently in reminiscence of Stanley Kubrick's 60-year-old film satire "Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb," alluding to the nuclear annihilation stalemate in the Cold War. In response to his unusual choice of title, he told the audience about a meeting with representatives of Dutch intelligence services and their explanation that although they were not authorized to use their hacking tools to spy on fellow countrymen, they could provide other nations with investigative clues, for example on planned terrorist attacks or communication in organized crime networks , which has now led to an increasing number of raids and arrests in other countries . (ha) ÿ